Defense Against Weaponized Information:

A Human Problem,

Not Just A Technical One

by Nicholas J. Kane

> ***Social media manipulation will only get worse as artificial intelligence maps users' thoughts and arms propagandists with unprecedented speed and the power to endlessly amplify their message.***
>
> ***—Clint Watts, "Messing with the Enemy"***

> ***The best protection against threats to the cognitive dimension of cyberspace depends on users' own actions and knowledge. Objectively educated, rational citizens should serve as the foundation of a strong democratic society. But that defense fails if people don't have the skills—or worse, don't use them—to think critically about what they're seeing and examine claims of fact before accepting them as true.***
>
> ***—Richard Forno, "Weaponized information seeks a new target in cyberspace: Users' minds"***

In the Information Age, near-infinite data is available with just a few clicks of a mouse. Furthermore, users, wittingly or unwittingly, offer up much personal information that a person, with some basic computer skills and a few social media personae, can access, aggregate, and exploit. Scandals, like the Cambridge Analytica exposé and the discovery of the Russian internet troll-farm – the innocuously named Internet Research Agency – meddling in 2016 U.S. Presidential election demonstrate that "big data" can be a threat to U.S. national security. Additionally, these two instances highlight how, through the aggregation of open source information on the internet, criminal elements, and adversary governments can weaponize information in pursuit of financial gain or political objectives. There is significant, aggressive competition between states that do not cross the threshold into declared armed conflict, such as malign influence and nefarious actions in the information environment – to include cyberspace – that impinge upon the sovereignty of states.

Unfortunately, current international laws and conventions do not satisfactorily account for

Major Nicholas J. Kane holds a Master of Military Arts and Science and a Master of Arts in Military Operations from the U.S. Army Command and General Staff College, where he was an Art of War Scholar and a graduate of the School of Advanced Military Studies. Kane also has a Master of Science in adult learning and leadership from Kansas State University.

undeclared conflict and non-lethal effects on civilians and states. Under these international laws, cyber intrusions, and weaponized information in the "gray zone" short of armed conflict do not present as clear-cut justification for the use of military force within the Just War theory. This legal murkiness presents Western democratic states with a dilemma: operate aggressively in the information environment and stem the onslaught of malicious activity or maintain the moral high ground. If the United States attempts to seize the initiative offensively with weaponized information to abate the threat from adversaries, it risks losing legitimacy of narrative in the international community. Should the status quo remain, the United States risks fracture of internal and external security relationships and will continue to experience malign foreign influence in its society, which causes divisiveness and discord. Therefore, to maintain public trust and international legitimacy, the U.S. military should only employ certain types of weaponized information, especially targeting civilians, in steady state competition as a means of strategic defense. However, there must be a codified threshold in which Western powers will openly leverage all forms of weaponized information aggressively during limited wars or in the event of declared large-scale armed conflict.

Using political warfare via social media and other internet outlets, Russia covertly exposed harmful information in conjunction with disinformation for a greater effect to impact the outcome of the U.S. election to foment discord in American society and undermine the trust in its democratic processes.[1] Furthermore, the Russo-Ukrainian conflict showcased Russia's willingness to leverage weaponized information against military and civilians alike in pursuit of military objectives. During major combat in Ukraine, military propagandists delivered false and demoralizing messages to Ukrainian soldiers at the front and their family members back home via cyber-electromagnetic means.[2] Thus, malicious state and non-states actors were targeting U.S. civilians, civilian infrastructure, and those of our allies domestically and abroad.

...to maintain public trust and international legitimacy, the U.S. military should only employ certain types of weaponized information...

With adversaries focused on the cognitive dimension of the information environment within democratic and open societies, multiple questions arise. First, are there forms of weaponized information that are more acceptable for employment than others? Second, can the United States employ weaponized information within Just War theory? Finally, is it ethical to target civilians associated with the military?

Giulio Douhet and other theorists of warfare would likely argue that when targeting the morale and will of the people to support a government's pursuit of war, it could be a valid military target as a demoralized society would shorten the war, thus, saving lives. Additionally, Francis Lieber wrote General Order 100 in 1863, dubbed the "Lieber Code," which provided the foundation of the U.S. Laws of War and the Geneva Protocols. However, as a jurist, Lieber focused on the justice of actions in war, not the humanity of it.[3] Therefore, he might also agree that targeting civilians and family members with non-lethal efforts is permissible during a declared war. However, in the Information Age, declarations of war are less likely given the complex, interdependent character of the international political and economic systems.

What is Weaponized Information?

An element of "cognitive hacking," employing weaponized information means to "[bring] about a change in beliefs and attitudes and… promote behavior that serves the attacker's

purpose" and is designed to affect the target's cognition negatively.[4] In the strategic context, this definition places weaponized information into the category of "sharp power" which leverages soft power tools – like information– for nefarious purposes like deception and disinformation.[5] However, at operational and tactical levels during armed conflict, there is a difference between cyberwarfare, and information warfare conducted in cyberspace. In information operations, there are many information-related capabilities, but the five core information competencies are Operations Security, Electronic Warfare, Cyberspace Operations, Military Information Support Operations – formerly called psychological operations – and Military Deception.[6] Regarding Information Age warfare where cyberspace turned the globe into an information battlefield that ostensibly has no boundaries, P. W. Singer and Emerson Brooking codify five core principles in their book *LikeWar*:[7]

...Americans should have a vested interest in responsible online conduct, to consume content critically, and to be proactive in the security of their civilian information systems.

- "The internet has left adolescence."
- "The internet has become a battlefield."
- "The battlefield changes how conflicts are fought."
- "This battle changes what 'war' means."
- "We're all part of this war."

Using this logic, every user of the internet is now subject to information warfare. Additionally, war does not always mean bombs and bullets. Adversaries of the United States used this new paradigm of warfare to achieve political objectives while avoiding costly large-scale armed conflict. However, should states escalate to declared armed conflict, information warfare will still be a significant component of any war plan, and military personnel will not be the only targets, but rather the entire society. Therefore, given the current geopolitical climate, Americans should have a vested interest in responsible online conduct, to consume content critically, and to be proactive in the security of their civilian information systems.

Many laypeople assume that any activity in cyberspace constitutes cyber warfare, especially regarding social media. This assumption is not valid, at least from a military perspective. According to U.S. joint military doctrine for cyberspace operations:

> [C]yberspace is a medium through which **other information activities** and capabilities may operate. These activities and capabilities include, but are not limited to, understanding information, leveraging information to affect friendly action, supporting human and automated decision making, and leveraging information (e.g., military information support operations [MISO] or military deception [MILDEC]) **to change enemy behavior**.[8] (Emphasis added.)

For instance, in 2019, the North Atlantic Treaty Organization's (NATO) Strategic Communications Centre of Excellence conducted a study in which researchers leveraged publicly available information and social media platforms to "instill undesirable behavior" in military personnel actively participating in a military exercise.[9] According to a *Business Insider* report, the researchers accomplished this result for less than $60.[10] Now imagine what a state-sponsored entity can accomplish in the cognitive dimension with resources available to a former superpower that has over 100 years of practice in the art of

propaganda and disinformation. As of early 2019, the Russian military viewed open source information on the internet and social media platforms as such a significant risk that Russia instituted policies and laws banning the use of social media by active soldiers. "Soldiers' social media data has allowed open-source journalism sites like Bellingcat to expose secret military activity by Russian forces, sometimes in real time."[11] Thus, reinforcing the assertion that the internet and social media pose tactical and operational risks for soldiers, as well as political risks for the state.

There are four general kinds of weaponized information: exposed truths that are damaging, amplification of half-truths and misinformation, complete falsehoods and disinformation, and technical information. First, harmful truths must be detected, identified, and exposed or compromised at a specific time and medium to achieve the most impactful effect. Typically, actors collect this type of information on individuals and organizations to alter public perceptions of those entities.

Second, half-truths and misinformation can be a hybrid of truths and plausible, but ambiguous embellishments or truths conveyed out of context in a manufactured "reality" that credible outlets may amplify and give it legitimacy. This kind of weaponized information can be the most damaging as it is capable of reaching the greatest audience because of the semi-truthfulness and plausibility of the whole story based on the veracity of a piece of it, whereas audiences can be more readily dismiss exposed truths and manufactured lies as adversary propaganda.

Third, outright falsehoods and deception are fabricated stories and information. The purpose of deceptive content is to create and exacerbate rifts among groups within a society or to cause decision makers to act or take inaction as the content originator desires. For this type of content to be effective, the information must be plausible or already fit into the audiences' biases. However, if the information is too outside the norm for that non-critically thinking audience, it risks dismissal as propaganda.

There are four general kinds of weaponized information: exposed truths that are damaging, amplification of half-truths and misinformation, complete falsehoods and disinformation, and technical information.

Finally, on the technical side of this examination, are the systems and software designed for malicious purposes such as ransomware, botnets, and other malware. From computer software code to external physical devices, hackers and other agents can introduce means to disrupt, deny, degrade, manipulate, or destroy aspects of cyberspace. These effects translate into temporary or permanent damage to information and infrastructure, and as second or third orders of effect, cognitive damage of the intended target or audience.

A critical element of the offensive use of information is the intelligence apparatus. Intelligence collection is critical as it provides the raw information that planners weaponize to achieve or maintain a relative advantage over an adversary. Not only do intelligence entities seek protected, sensitive information, but they can aggregate seemingly innocuous data that is publicly available or relatively easy to access via the open internet. Therefore, Americans must revisit how they guard their personal information.

How do adversaries employ this information? Sebastian Bay and Nora Biteniece highlight four ways in which malicious actors can use data: manipulation, impersonation, exposing sensitive information, and doxing.[12] Manipulation refers to the alteration of data resident in various systems in databases after

malicious actors gain access to them.[13] Bay and Biteniece describe possible effects of how cyber intrusions to manipulate information or processes that result in "inaccurate data [which] could prevent a person from securing a loan or being granted a security clearance. Inaccurate data can cause an [organization] to make erroneous decisions and lost data can be difficult or expensive to replace."[14] Impersonation is when an actor has aggregated enough personal data about an individual that it is possible to determine passwords and hack into online personae or to generate a new cyber-persona in the individual's name for nefarious purposes.[15] In these instances, the malicious actors primarily seek the secondary or tertiary effects of the act, such as or gaining placement and access in cyberspace for future wider dissemination of misinformation or deceptive content.

...doxing...is "the technique of intentionally releasing selected sensitive information about an individual...

Another method an adversary can employ is doxing, which is "the technique of intentionally releasing selected sensitive information about an individual to influence public perception of that individual, or the creation of conditions and vulnerabilities that can be exploited."[16] The Wikileaks releases about surveillance on Allies to cause or exacerbate rifts in NATO, or the hacking of the Democratic National Committee emails during the 2016 U.S. Presidential elections are examples of doxing. Within the military, this could involve exposing inappropriate or seemingly questionable behavior of key personnel within an organization, which has disruptive effects both up and down the chain of command and degrade cohesion and readiness of units. Finally, exposure of sensitive information like the location and character of operational or clandestine activities, such as the Russian servicemembers in Crimea, increases the military and political risk and may result in the loss of initiative in the information environment. In these instances, the desired first order effect is exposure and compromise, which can lead to going viral when "useful idiots" reshare, retweet, or mainstream media picks up the story and amplifies the information to a much wider audience from a seemingly legitimate platform.

Armed with these tools and methods, adversary actors can detract from the U.S. military's readiness to perform its duties of national defense. All that an intelligence entity within an adversary security apparatus needs to find are small pieces of information to exploit can detract from the readiness of a particular soldier or unit before or during deployments. For example, infidelities of soldiers, existing interpersonal rifts within a unit or community, or illicit behavior are all lucrative instances for foreign intelligence entities seeking to disrupt cohesion within a unit overseas and on the Homefront. Other targets could include the Defense Enrollment Eligibility System and Tricare websites and other military support systems that also enable provision of services for servicemembers, retirees, and family members. Are these valid military targets?[17]

As mentioned, the Russians employed such techniques in Ukraine with text messages to Ukrainian soldiers and their family members. Does this activity, in this case, cross a line of criminality from intimidation, blackmail, and extortion to a valid technique for the U.S. military during large-scale combat? If legal, although morally reprehensible, is this activity something that should be retained with the special operations community or become a practice for conventional forces if operationally feasible?

Legality versus Ethics

Legality and ethicality are not necessarily synonymous. An act may be legally permissable,

but unethical or immoral at the same time. While laws and codes of ethics are essentially agreed upon normative behaviors, Russell Dipert proffers that set normative behaviors and concepts of ownership –like the notion of a state's sovereignty after the 1648 Treaty of Westphalia – took centuries to develop and the normalization of ethical and legal behavior and ownership in cyberspace is still woefully underdeveloped.[18]

From a moral, emotional perspective, use of weaponized information offensively, especially against civilians, causes outrage in a democratic free society. This outrage begs another question. For example, in a society that deemed the Stolen Valor Act – which made it illegal to impersonate or make false claims about military service – unconstitutional, as it violated the right to free speech, is it illegal to disseminate knowingly false and harmful information? The U.S. Supreme Court protected deliberately false information as free speech – so long as there are no material and financial gains as a result of that falsehood. Hence, the act of lying is legal, but unethical and immoral. Ultimately, it depends on the intent and desired effect of the act in context to determine the morality, and ethicality of a legal act.

In a time of declared armed conflict, the legal status of certain actions changes within a mutually agreed upon set of normative behaviors to justify those actions. These normative behaviors are the rules of war that the international order codified. However, information warfare, including cyberwarfare, do not constitute armed conflict despite the weaponization of information and ideas. As the traditional legal frameworks do not recognize malign information and data employed in cyberspace as "armament," limiting deterrent and response options of a state that is a victim of aggression, intrusions, and attacks in cyberspace — unless physical damage that impacts its citizenry results.[19]

Efforts to codify normative behavior in cyberspace began in the 2000s, but is not nearing a good solution in the near-term, especially with the rapid rate of technological advancements. Cyber-ethics scholar George Lucas attributes some of the lack of significant progress to the fact that "[c]ontributors to the *Tallinn Manual* chose to focus their efforts on the interpretation of *extant legislation*, rather than advocating new law or international treaties."[20]

...use of weaponized information offensively, especially against civilians, causes outrage in a democratic free society.

Thus, the document lacked the teeth to account for the new realities of modern technology and the geopolitical climate. Additionally, the predominantly NATO group that deliberated in Tallinn did not include Russian or Chinese representation – two of the significant actors in cyberspace – which was a missed opportunity to engage in dialogue with two current threat actors and begin to determine new normative behavior in cyberspace.[21] Therefore, while discussions continue on the topic, the international community has not agreed upon a set of normative behaviors in cyberspace.

Imagine a scenario in which a civilian receives a text message or logs into social media to discover that a loved one serving in the military abroad is dead or critically wounded; or a scenario in which a military servicemember in rear areas of a battlefield receives word that his or her spouse has left or that a child was injured. This servicemember has been the target of weaponized information, and its disruptive effects detract from the servicemember's focus and degrade morale. Does this type of activity qualify as terrorism – seeking to achieve change and outcome using fear – under International Humanitarian Law and does this violate the myriad conventions that are supposed to protect

civilians by espousing discrimination and non-combatant immunity during a war? What if international armed conflict is not declared, are civilians still protected in this case? Do those conventions apply to lethal targeting and suffering of civilians and servicemembers— or is psychological suffering included in the intent and interpretation of the laws?

Just War Theory and Weaponized Information: *Jus Ad Bellum* and *Jus in Bello*[22]

Thomas Aquinas, Hugo Grotius, and Emer de Vattel were philosophers in the thirteenth, seventeenth and eighteenth centuries, respectively, whose writings provided the foundational framework of a codified Just War theory.[23] Simply put, there are three primary facets that comprise Just War theory: *jus ad bellum*, the justification for using military force; *jus in bello*, just conduct in war; and *jus post bellum*, just peace. However, if cyberspace and social media have recast societies and the character of warfare, how does Just War theory apply in the Information Age? While *jus post bellum* is significant to the spectrum of conflict and peace, *jus ad bellum* and *jus in bello* hold the most relevance to the aim of this examination. While Lucas and other scholars opine that the traditional Just War theory is insufficient in modern information warfare, no widely accepted replacement exists in the literature.[24] Therefore, this examination leverages the current Just War tradition to describe ethical considerations of using weaponized information during and outside of declared armed conflict.

Russia, China, Iran, and North Korea push the boundaries of information warfare...

The first facet of Just War theory, *jus ad bellum*, is primarily the domain of politicians and strategic thinkers that influence decisions on whether to enter into declared armed conflict based on four criteria: just cause, last resort, the probability of success, and proportionality.[25] The three most relevant aspects of this facet of Just War theory are just cause, last resort, and proportionality. These principles of directly link to the decision to leverage military force against an adversary and the framework for the argument lies within International Humanitarian Law. Decision makers derive the lawful use of military force from the Geneva Conventions of 1949, two subsequent Additional Protocols from 1977, and the United Nations Charter.

With the actions already discussed about cyberspace and the wider information environment, Russia, China, Iran, and North Korea push the boundaries of information warfare in pursuit of strategic aims without crossing the threshold of escalation to major armed conflict. These states, as well as violent extremist organizations, exploit open press in democracies and they dominate their own information environments, which make those environments difficult for the United States to affect. Until recently, the cyber strategy of the United States was defensive and reactive after attacks rather than proactive to prevent adversary cyber-attacks. Now, the Department of Defense and the U.S. Cyber Command has altered the status quo and seeks to change the paradigm within which adversaries operated. The strategic messaging began in September 2018 with the release of the *Department of Defense Cyber Strategy* and continued in March 2019 when General Paul Nakasone, the commander of U.S. Cyber Command, conducted an interview and published an article in *Joint Forces Quarterly*.

In the summary of the 2018 *Department of Defense Cyber Strategy*, the United States took a bold step and introduced the "defend forward" concept.[26] This concept essentially means that if the intelligence community observes credible indications and warnings that foreign cyber

actors intend an imminent attack, then the Department of Defense can preemptively execute activities in cyberspace to disrupt that attack to protect the Defense Industrial Base. This tactic is akin to the spoiling attack of the traditional battlefield which seeks to "disrupt enemy's troop concentrations and attack preparations" and "allows the defending force to regain the initiative."[27]

Additionally, General Nakasone reinforced the "defend forward" concept and introduced the strategic concept of "'cyber persistence' rather than 'cyber response.'"[28] These new strategic concepts demonstrate the United States government is comfortable with U.S. Cyber Command operating with fewer restraints in the strategic information environment. This change in policy is possibly due to operational successes, the maturation of the command, and expanded working relationships with other government agencies and allies. Regardless of the impetus, the changes mean that adversaries cannot continue to operate as freely in cyberspace as they had before.

The other facet of Just War theory, *jus in bello*, has three main principles that include proportionality, discrimination, and military necessity. All three are rich for discussion of the employment of weaponized information. First, proportionality "concerns how much force is morally appropriate" and refers to the estimation of intended good achieved as an outcome of a military action compared to the anticipated harm said action would likely cause.[29] Much in line with the *jus ad bellum* debate on whether cyberattacks that steal information or disrupt or degrade critical systems provide justification to attack the responsible actor with military force, so too is there a jus in bello discussion of proportionality regarding cyber actors and use of lethal force.

Under the principle of proportionality, a dilemma arises about whether to use lethal force against cyber actors or those propaganda media entities that terrorize civilians and soldiers, or those who promote ideologies that result in terrorism and atrocities. Ideas like the Islamic State's brand of Islam was weaponized and used to radicalize at-risk populations in the United States and abroad to inspire "lone wolf attacks" of terrorism in Western states. The U.S. military deemed, likely using the principle of military necessity, that the use of lethal force against such entities is permissible, demonstrated by the killing of a French citizen in February, 2019 who functioned as an ISIS propagandist in Syria.[30] The need to prevent ISIS propaganda from terrorizing French citizenry with weaponized information could contribute to the future determination that lethal force against adversary information warfare specialists is acceptable as a normative proportion of lethality for protecting civilians against dangerous ideologies and propaganda.

...the United States government is comfortable with U.S. Cyber Command operating with fewer restraints...

Next, discrimination "concerns who are legitimate targets in war."[31] The targeting of civilians with weaponized information is the crux of this examination. The targets that actors leverage weaponized information against are individuals and organizations in the cognitive dimension, and infrastructure in the informational and physical dimensions of the information environment. Ultimately, information activities are to shape perceptions, behaviors, and decisions of the targets. Information Age competition seeks warfare that is of a lesser form than that of traditional warfare of the twentieth century.

Per Colm McKeogh, author of *Innocent Civilians*, under a natural law-based approach, "suggested by [Hugo] Grotius and adopted by [Emer de] Vattel"- soldiers are "instruments

of the state."[32] However, McKeogh's research focused on formal war. Thus, the context of the Grotius and Vattel's assertions was of formally declared war, given the contemporary paradigm of warfare. Would these philosophers accept that volunteer soldiers in a standing military outside a state of war constitute valid targets of non-kinetic activity? McKeogh highlighted that soldiers were depersonalized instruments of the state because sovereigns pressed them into wartime service. Therefore, these men were not legally accountable for killing men because soldiers were instruments of war wielded by their sovereign.[33] Therefore, using logic, whether on duty or off, uniformed servicemembers are valid military targets in the Information Age, regardless if there is a declared armed conflict because information warfare falls below the currently accepted norms of *jus ad bellum*.

...explicit normative behaviors for undeclared conflicts...do not exist.

All the codified legal frameworks on warfare focus on normative behavior during declared conflict. However, explicit normative behaviors for undeclared conflicts like proxy wars and information warfare do not exist. While it may not be in the United States government's interest to establish new norms, and therefore, limit itself when it previous had a relative advantage, but earnest dialogue must continue between significant powers to move towards amelioration of these challenges. Until such time, the current law of armed conflict, International Humanitarian Law, and the Tallinn Manual are all there are to reference.

Published in 1863, Article 14 of General Order 100 – the Lieber Code – states that, "[m] ilitary necessity, as understood by modern civilized nations, consist in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war."[34]

Article 48—Basic Rule

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[35]

The first five points of Article 51 and the second point of Article 57 are also relevant to this examination as they more fully express the protection of civilians and the precautions that militaries must take during armed conflict. However, technological and societal progress in the forty-two years since these protocols took effect now provide challenges to the current context and character of competition and warfare.

Article 51—Protection of the civilian population

1. The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations. To give effect to this protection, the following rules, which are additional to other applicable rules of international law, shall be observed in all circumstances.

2. The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.

3. Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities.

4. Indiscriminate attacks are prohibited. Indiscriminate attacks are:

   a) those which are not directed at a specific military objective;

   b) those which employ a method or means of combat which cannot be directed at a specific military objective; or

   c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;

   and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

5. Among others, the following types of attacks are to be considered as indiscriminate:

   a) an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects; and

   b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[36]

Article 57—Precautions in Attack

[r]efrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be **excessive in relation to the** concrete and direct **military advantage anticipated**[.][37] (Emphasis added.)

In declared armed conflict, these rules explicitly apply to the conduct of war, but even so, these additional protocols to the Geneva Conventions of 1949 are specific to the treatment of civilians during war and in relation to military actions. Additionally, given the paradigm of warfare of the time, the implication about harm to civilians is that damage is physical, not necessarily cognitive. Therefore, the use of weaponized information against civilians, depending on the object of the act, is permissible in wartime.

...the use of weaponized information against civilians, depending on the object of the act, is permissible in wartime.

Additionally, if the non-military entities employ weaponized information in a declared conflict on behalf of the state, do these same laws apply? For instance, state intelligence entities or contractors could collect information, develop audience-specific content, and employ it without ever leveraging military means. Furthermore, not only does information warfare occur during armed conflict, but in the Information Age, it occurs as a part of statecraft in a new paradigm of warfare that is underdeveloped.

Finally, the Protocols are a codification of normative behaviors presented by an international organization that is not responsible for the enforcement of these codes of behavior. Theoretically, the United Nations Security Council is responsible for the enforcement of international humanitarian law. However, with Russia and China holding permanent membership on the council and veto power, it is unlikely that a resolution calling for enforcement of these codes would pass. Without a formal

declaration of war and a more effective version of the *Tallinn Manual*, authorities may only see malign activities in the information environment as criminal matters, rather than *jus ad bellum*. In the event of declared armed conflict, U.S. adversaries will likely find indirect ways to terrorize civilians with weaponized information in a manner to circumvent the intent of Article 51 of the Additional Protocols.

A significant element of the 2018 Department of Defense Cyber Strategy is the expression of responsibility of the Department of Defense towards the protection of the Defense Industrial Base.

For example, an instance in which civilians are targetable by adversaries in a declared armed conflict, despite the highlighted protections of the Geneva Conventions, is the Family Readiness Group. A Family Readiness Group is an official military entity and civilians who are associated with the military comprise it as family members of U.S. service men and women. The Family Readiness Group is an official entity because the company or battalion commander is responsible for the program and the group. The purpose of the group is to function as a mechanism for dissemination of information about the unit and the servicemembers' activity to facilitate expectation management and cohesion among the families. However, if online personae are injecting divisive messaging that could cause or exacerbate rifts within a Family Readiness Group, the community, or among soldiers, servicemembers and family members lose trust in the system, and the unit suffers.

Another example could be if adversary agents are posing as online love interests which could cause rifts between servicemembers that could affect morale and cohesion of a small tactical unit. As a result of the personal information internet users surrender to public availability as the price of entrance to the internet, adversaries can easily tailor personalized content to have the most impact on a targeted servicemember. Furthermore, adversaries can achieve significant effects with global reach in the cognitive dimension for little or no cost from the safety of strategic rear areas.

A third example or targeting civilians is adversary cyber actors attacking the previously mentioned support systems like the Defense Enrollment Eligibility System and Tricare. These systems support Department of Defense personnel, retirees, and their family members. Any disruption or denial of these services will have readily apparent operational effects on the Department, and the morale of its people.

A significant element of the 2018 Department of Defense Cyber Strategy is the expression of responsibility of the Department of Defense towards the protection of the Defense Industrial Base. The Defense Industrial Base is a loosely codified term that includes "Department, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements."[38] A key challenge with this new responsibility is whether the Department of Defense has the capacity to uphold its charge to protect the entire Defense Industrial Base. While the strategy signals that the DoD now has more granted authority to operate in cyberspace for national security, resources become a greater challenge given the additional responsibility.

Consequently, to accomplish the task of protecting the Defense Industrial Base, as well as the U.S. homeland, the Department of Defense will likely have to target civilian infrastructure in other states because that is where adversaries in cyberspace are operating. Thus, leading into the third principle of *jus in bello* – military necessity. Adversary cyberspace intrusions to gather

personal data for malign information activities and theft of defense-related information are current threats with which the Department of Defense must contend. Adversaries utilize the cyberspace domain for such espionage because it is cost-effective, it does not involve *physical* violation of sovereignty – reducing the risk to spies of capture – and attribution of the act is often difficult to discern. Additionally, cyberspace is the domain of social media which means that, in a society that values freedom of speech and open press, the United States and Western democratic societies are especially vulnerable to information warfare. Is our society resilient enough to withstand an onslaught of weaponized information tactics, especially in the event of a declared armed conflict?

The military necessity of targeting civilians with information is controversial but justifiable in that, from a Western democratic worldview, the principle of noncombatant immunity, while not absolute, should hold true in declared armed conflict. In the principle of "double effect, the primary determinant of the moral quality of an act is the intention...There is an important moral distinction between intention and foresight."[39] Therefore, despite the legality of an action during declared conflict under the principle of military necessity, decision makers must weigh the morality of the proposed action with the potential consequences.

For military leaders in armed conflict, ethical dilemmas arise in the operational environment, which includes the information environment, that do not present clear-cut "right" answers, but rather "less wrong" answers. Simply because an actor in wartime *can* conduct an action does not necessarily mean that actor *should* execute that action. Therein lay dilemmas for military commanders.

There are three lenses through which to view ethical dilemmas. First, there is a principles-based approach which refers to codified normative behaviors and laws. Second, morality enters the discussion in the values-based approach. Finally, the utilitarian approach, also called the consequentialist approach, stems from a perspective based on intent and outcomes.[40] The weighing of each of these perspectives in context of the dilemma is what David Fisher calls "virtuous consequentialism," which he highlights, "insists, if we are to account for the complexity and richness of our moral lives, each of these features – intentions, rules, consequences, and virtues – needs to be given appropriate weight."[41] Essentially, each context is unique and military decision makers will have to consider the legal and moral implications of potential courses of action weighed against the intent of the actions and the foreseeable outcomes.

The military necessity of targeting civilians with information is controversial but justifiable...

For example, employing weaponized information to expose malign activity is laudable if the object is the pursuit of truth and preventing further aggression in the information environment. The Bellingcat exposure of the Russian shootdown of flight MH 17 over Ukraine is an example of weaponizing information for good, despite the negative consequences for Russia. However, using false information or weaponized truths to spread terror, to demoralize civilians, or compel action or inaction by decisionmakers becomes more challenging to justify ethically, despite the legal permissibility. The double effect principle is consequentialist in character in that foreseeable negative outcomes are morally and ethically permissible as long as the intention of the act was ultimately for good in relation to the harm caused.

Ultimately, civilians, even those associated with the military, should not be the object of weaponized information with the intention of

terrorizing them. While the protections obligated to civilians under the Additional Protocols were a means to prevent unnecessary physical suffering of civilians, their psychological suffering is implicitly protected by ethically behaving militaries. However, civilians are targetable in wartime in terms of information gathering to facilitate greater effects on adversary decision makers. Some civilians such as family members, friends, and associates can serve as vectors and conduits when friendly forces cannot deliver or project information directly to a targeted military individual.

...Voice of America is already in use to promote Western democratic ideals and expose malign influence with truthful information...

The United States strives to maintain the high moral ground in the international arena, especially in the information environment. The 2017 U.S. National Security Strategy states:

> [The United States] will continue to champion American values and offer encouragement to those struggling for human dignity in their societies. There can be no moral equivalency between nations that uphold the rule of law, empower women, and respect individual rights and those that brutalize and suppress their people. Through our words and deeds, America demonstrates a positive alternative to political and religious despotism.[42]

However, the reality of the geopolitical climate will require the United States to engage adversaries aggressively in the information environment if threat levels increase above certain thresholds. Hence, virtuous consequentialism becomes an apt framework for decision-making in a war in the realities of the Information Age.

Thresholds of Employing Information

If Western societies value open press and free information while adversarial authoritarian regimes control their domestic information environments, then democracies are more vulnerable to weaponized information. A way to overcome this challenge is to develop new ways to project internet capability into environments where the state limits the internet service provider and "throttles" certain areas or users from access. The United States cannot cognitively affect an adversary's society easily if it cannot interact with the target informational environment.

In the current steady state, Voice of America is already in use to promote Western democratic ideals and expose malign influence with truthful information, as are each military combatant command's public affairs activities. Additionally, the Global Engagement Center within the Public Diplomacy section of the Department of State has the responsibility of countering adversary propaganda. After the U.S. Information Agency dissolved in 1998, many of the functions of that agency transferred to the Department of State.[43] However, the Global Engagement Center is woefully underfunded to achieve notable success in the task to which it must execute. In December 2016, President Obama approved the 2017 National Defense Authorization Act in Section 1287 authorized appropriation of $80 million toward the effort for 2017, and again in 2018, with authorization for the Department of Defense to transfer up to $60 million of its budget.[44] In 2018, the Department of Defense was reportedly to transfer $40 million to the Department of State.[45] The Global Engagement Center's task is also very reactive, whereas U.S. CYBERCOM's newly announced "defense forward" and "persistent presence" strategic concepts are more proactive and authorize the Department of Defense to act preemptively and preventively.[46]

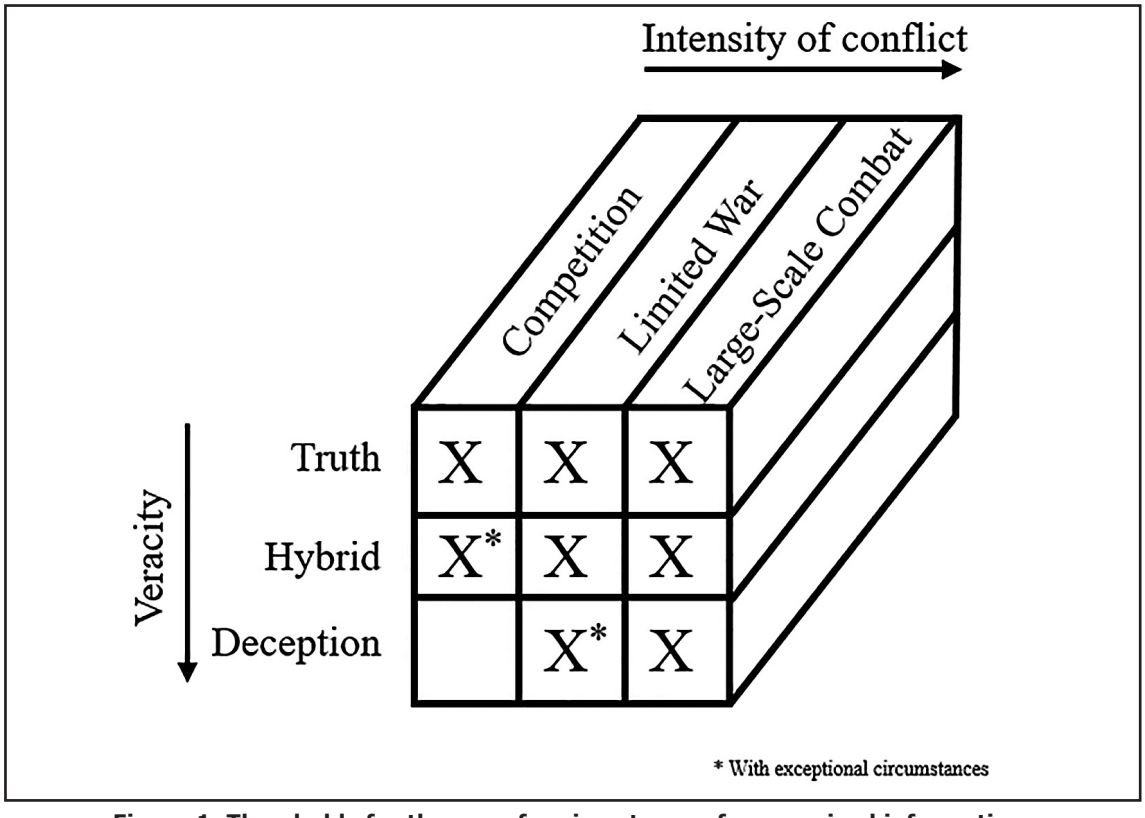

Figure 1. Thresholds for the use of various types of weaponized information.
Source: Created by author.

In limited wars, like the Balkan conflict in the 1990s and the Global War on Terror, against state and non-state actors, the United States military targeted civilian populations with information as well. In the event of large-scale combat operations, akin to the total wars of the 19th century, the United States and its Western allies must determine the level of political risk they will accept to conduct operations in the information environment, especially when targeting civilians. Figure 1 depicts a conceptual escalation of when military entities should have the authorization to leverage the various types of weaponized information. Not included in this particular figure is malicious code and software which affects cyberspace systems. Instead, this figure seeks to convey when conventional military entities should use these types of information. The asterisk denotes instances when special operations or other military activities could employ the type of weaponized information indicated, rather than traditional military units.

For instance, during the competition phase, the military should leverage truthful information to achieve its objectives, or degrade an adversary's ability to achieve its aims, such as exposure of malign activity by adversaries. While certain situations short of declared armed conflict may arise wherein special operations granted by expanded authorities in the information environment may be necessary, the military should not leverage completely false weaponized information activities. Rather, entities that comprise other instruments of national power may or may not do so as they are unconstrained by the authorities granted under Title 10 of the United States Code, which dictates what the U.S. Armed Forces must do, and the restraints they must observe. This

restraint of the military is critical to maintaining the public trust, domestically and internationally.

Conclusion

While cyberspace entities and activities primarily represent the technological side of information warfare, and other information-related capabilities strive to achieve effects in the cognitive dimension of the information environment, the two are not mutually exclusive of one another. While there exists both human and technical problems in modern warfare and inter-state competition, most of the solutions reside in the people who comprise the military and society, rather than reliance upon materiel and technical solutions only.

Ultimately, although the United States Department of Defense and Western military powers should only leverage truthful weaponized information in steady state competition, they must be ready to operate more aggressively in the information environment should an armed conflict arise. The military must be ready, behaving within virtuous consequentialism and the "double effect," to ethically target military and civilians with weaponized information to preserve stability as a preemptive, protective measure, or reestablish a secure peace in the event of armed conflict. However, the use of weaponized information by the military cannot be for the sole purpose of terrorizing civilians, in accordance with the spirit of the intent of the Additional Protocols.

George Kennan, in his analysis of the Soviets that led to the Cold War containment strategy, said that "[t]o avoid destruction the United States need only measure up to its own best traditions and prove itself worthy of preservation as a great nation."[47] Joseph Nye offered similar advice when he said, "…democratic government and societies should avoid any temptation to imitate the methods of their adversaries."[48] Both Kennan and Nye across the ages opined that the United States should never stoop to its adversary's level – i.e., Russia – when conducting such activities in warfare. However, could such an existential crisis emerge where it becomes necessary to engage or employ said option that may detract from Western democratic values and legitimacy narrative in order to ensure survivability of the nation? If the United States holds true to its core values, then it must find ways to build a more resilient society to adversary information warfare.

Currently, technological solutions contribute most to the protection of U.S. society from the combined efforts of the U.S. CYBERCOM and National Security Agency within the Department of Defense, the Central Intelligence Agency, the Department of Homeland Security, and the Department of Justice – notably the Federal Bureau of Investigation. These departments and agencies identify and mitigate threats. However, to truly develop cognitive resilience against weaponized information, Western societies must relook how they educate their publics on responsible online conduct, and continue to pursue policy and regulation of the commercial sector with regard to the protection of citizens' privacy. Furthermore, national security entities must strive to regain or retain the initiative in the information environment.

Recommendations

Since adversaries of the United States continue to demonstrate a willingness and capacity to employ both truthful and false information against Western powers, servicemembers and units must develop policies and practices to facilitate resilience to weaponized information and cognitive attacks. The world has come far since the mid-nineteenth century regarding the laws of war, but with technological advancement occurring so rapidly under Moore's Law, it is struggling to keep up. Therefore, it is ultimately up to each individual to provide self-protection through identity management and responsible online behavior

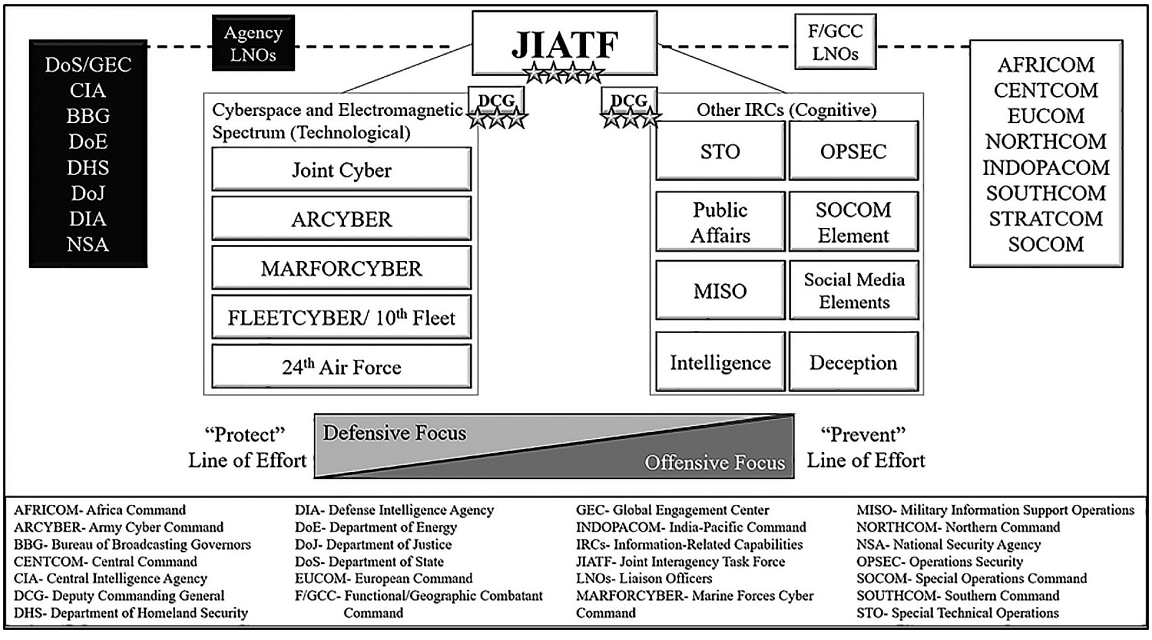

Figure 2. Notional military-led joint interagency task force for operations in the information environment in steady-state competition.[50]
Source: Created by author.

until governments can catch up. Identity management and media literacy education are key recommendations for resilience against the demonstrated adversary information tactics.

The author previously recommended the establishment of a Joint Interagency Task Force (JIATF) to undertake two lines of effort against adversary information warfare: to protect and to prevent.[49] Figure 2 depicts a notional concept for a military-led JIATF that leverages military information capabilities in concert with other government agencies that directly or indirectly contribute to the informational instrument of national power. Whichever department or agency leads the task force depends on the context of the JIATF's establishment and its purpose.

This conceptual JIATF resembles U.S. CYBERCOM to a degree, given the current purview of that combatant command in cyberspace and in light of the recent interagency efforts to prevent or mitigate foreign meddling in the 2018 midterm elections. The JIATF in this conception is appropriate for steady-state competition, but in the event of a limited conflict, or large-scale combat, a different variation in size or composition may be necessary. For example, U.S. CYBERCOM established Joint Task Force Ares to "defeat of the [so-called Islamic State] in virtual space."[51] Another example that General Nakasone highlights in a *Joint Forces Quarterly* interview is the Russia Small Group, a "[U.S. CYBERCOM/National Security Agency] partnership to assist in the securing of the 2018 mid-term elections."[52]

While the Protect line of effort involves technical solutions for monitoring and responding to threats, the human dimension of the problem and potential solutions require attention. For instance, monitoring of the domestic population, especially in the post-Snowden leak era, increases sensitivities about civil rights. Additionally, during a conflict, the Prevent line of effort must address the ethics of targeting of civilians with weaponized information of varying type to

Education and monitoring are elements of the Protect line of effort and while feasible for the military, for the most part, to apply the

concept to American society would be impossible in the current paradigm. First and foremost, the military can direct all personnel to partake in additional education and training to defend against weaponized information, but the federal government can only apply so much leverage to how states manage education for the civilian population before negative sentiment arises about the level of federal government interference. While the military can control how its information systems operate and dictate terms of usage to its servicemembers, contractors, civilian employees, the family members of these people are under no obligation to use the internet and other civilian information systems in any government dictated manner – except for illegal behavior. This same challenge applies to personnel within the loosely defined terms of the Defense Industrial Base.

Internationally, diplomats, jurists, and ethicists should continue to engage in dialogue pursuant to codifying normative behaviors regarding cyberspace and information warfare. A key challenge is that major relevant actors may not find it in their best interest to limit themselves in the information environment as they currently hold some form of relative advantage. Another significant challenge to overcome is empirically measuring psychological effects and harm. The difficulty is proving harm, and attribution of the source of the harm which makes it near impossible to hold an actor accountable – even if the actor is a signatory of an agreed upon convention or treaty.

These recommendations are not quick solutions. Technological solutions are relatively fast, and somewhat measurable in demonstrating quantifiable effects, whereas changing the cognitive dimension within societies takes a long time and is difficult to measure and prove causality because humanity is complex. Regardless of how difficult it will be to influence a cognitive shift in the United States, society must begin taking steps now to generate momentum in achieving long-term effects. ***IAJ***

NOTES

1 Alina Polyakova and Spencer P. Boyer, *The Future of Political Warfare; Russia, the West, and the Coming Age of Global Digital Competition* (Washington, D.C.: Brookings Institute, 2018), 5-9.

2 Aaron F. Brantly, Nerea M. Cal, and Devlin P. Winkelstein, *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW* (West Point, NY: Army Cyber Institute, 2017), 28.

3 John Fabian Witt, *Lincoln's Code: The Laws of War in American History* (New York: Free Press, 2012), 178.

4 Margaret Rouse, *TechTarget*, accessed 16 March, 2019. https://whatis.techtarget.com/definition/weaponized-information.

5 Joseph S. Nye Jr., "How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence," *Foreign Affairs*. 24 January, 2018, accessed 22 April, 2018. https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power.

6 Department of Defense, Joint Publication 3-13, *Information Operations* (Washington, D.C.: Government Printing Office, 2006), VII-1.

7 P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt Publishing, 2018), 21-22.

8 Department of Defense, Joint Publication 3-12, *Cyberspace Operations* (Washington, D.C.: Government Printing Office, 2018), I-7.

9 Sebastian Bay and Nora Biteniece, "The Current Digital Arena and its Risks to Serving Military Personnel" in *Responding to Cognitive Challenges*. Accessed 17 March, 2019. https://www.stratcomcoe.org/current-digital-arena-and-its-risks-serving-military-personnel.

10 Ryan Pickrell, "Researchers Found and Tracked NATO Troops and Tricked Them into Disobeying Orders for just $60," *Task & Purpose*. 19 February, 2019. Accessed 20 February, 2019. https://taskandpurpose.com/researchers-track-nato-troops-internet.

11 BBC News, "Russia bans smartphones for soldiers over social media fears," *BBC News*, 20 February 2019. Accessed 21 February, 2019. https://www.bbc.com/news/world-europe-47302938.

12 Bay and Biteniece, 11.

13 Ibid.

14 Ibid.

15 Ibid.

16 Ibid.

17 The Defense Enrollment Eligibility Systems (DEERS) is a database of information on uniformed services members (sponsors), U.S.-sponsored foreign military, DoD and uniformed services civilians, other personnel as directed by the DoD, and their family members. Personnel must register in DEERS to get access to TRICARE, the health insurance service.

18 Randall R. Dipert, "Distinctive Ethical Issues of Cyberwarfare," *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (New York: Oxford University Press, 2016), 67.

19 Ibid., 62.

20 George R. Lucas, Jr., "Emerging Norms for Cyberwarfare," in *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (New York: Oxford University Press, 2016), 17.

21 Ibid.

22 For additional information on the historical underpinnings of Just War Theory, see Gregory M. Reichberg et al., *The Ethics of War: Classic and Contemporary Readings*, and Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*.

23 Gregory M. Reichberg, Henrik Syse, and Endre Begby, *The Ethics of War: Classic and Contemporary Readings* (Malden, MA: Blackwell Publishing, 2006), 70, 168, 385, and 504.

24 George R. Lucas, Jr., *The Ethics of Cyberwarfare: The Quest for Responsible Security in the Age of Digital Warfare* (New York: Oxford University Press, 2017), 41.

25 James Fieser, "Just War Theory," *Internet Encyclopedia of Philosophy*, (University of Tennessee at Martin). Accessed on 1 December, 2018. http://www.iep.utm.edu/justwar.

26 Department of Defense, *Summary of the Department of Defense Cyber Strategy, 2018* (Washington, D.C.: Government Printing Office, 2018), 1.

27 Department of the Army, Army Doctrine Reference Publication 3-90, Offense and Defense (Washington, D.C.: Government Printing Office, 2012), 4-10.

28 Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly*, no. 92 (1st Quarter 2019): 10-14, 12.

29 Fieser. Accessed on 1 December, 2018. http://www.iep.utm.edu/justwar.

30 Elian Peltier, "Fabien Clain, Prominent French Voice of ISIS, Is Reported Killed in Syria," *New York Times*, 28 February, 2019. Accessed on 26 March, 2019. https://www.nytimes.com/2019/02/28/world/europe/fabien-clain-death-isis-france.html.

31 Ibid.

32 Colm McKeogh, *Innocent Civilians: The Morality of Killing in War* (New York: Palgrave, 2002), 120.

33 Ibid.

34 Witt, *Lincoln's Code*, 377.

35 International Committee of the Red Cross, *Protocol Additional to the Geneva Conventions of 12 August 1949*, 8 June, 1977, 36. Accessed 24 March, 2019. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf.

36 Ibid., 38.

37 Ibid., 42.

38 Department of Defense, *Summary of the Department of Defense Cyber Strategy, 2018*, 3.

39 David Fisher, *Morality and War: Can War be Just in the Twenty-first Century?* (Oxford, UK: Oxford University Press, 2011), 86-87.

40 Jack Kem, "The Use of the "Ethical Triangle" in Military Ethical Decision Making," *Public Administration and Management*, 11, no. 1: 22-43.

41 David Fisher, *Morality and War: Can War be Just in the Twenty-first Century?* (Oxford, UK: Oxford University Press, 2011), 135.

42 Donald J. Trump. *National Security Strategy of the United States of America*. (Washington, D.C.: White House, 2017), 37.

43 U.S. Congress. House. *Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment*. Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, 115th Cong., 1st Sess., 15 March 2017, 82.

44 U.S. Congress. House. Committee on Armed Services. *National Defense Authorization Act for Fiscal Year 2017* (Washington, D.C.: Government Printing Office, 2017); https://www.portman.senate.gov/public/index.cfm/2016/12/president-signs-portman-murphy-counter-propaganda-bill-into-law.

45 Department of State. "State-Defense Cooperation on Global Engagement Center Programs and Creation of the Information Access Fund to Counter State-Sponsored Disinformation," Press Release, February 26, 2018. Accessed on 5 April, 2019. https://www.state.gov/r/pa/prs/ps/2018/02/278851.htm; Joel Gehrke. "Pentagon, State Department launch $40 million counter-propaganda effort aimed at Russia," *Washington Examiner*, February 26, 2019. Accessed on 5 April, 2019. https://www.washingtonexaminer.com/pentagon-state-department-launch-40-million-counter-propaganda-effort-aimed-at-russia.

46 Department of Defense, *Summary of the Department of Defense Cyber Strategy, 2018* (Washington, D.C.: Government Printing Office, 2018), 1.

47 George F. Kennan, "The Sources of Soviet Conduct," Foreign Affairs, (1947): 566-582, 582.

48 Joseph S. Nye Jr., "How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence," Foreign Affairs. 24 January, 2018, accessed 22 April, 2018. https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power.

49 Nicholas J. Kane, "Will Russian Exploitation of Open Press Destroy U.S. Democracy?" *InterAgency Journal*, vol. 9, no. 3 (Fort Leavenworth, KS: CGSC Foundation, 2018): 69-74, 72.

50 I adopted this figure from an original proposal I made about restructuring U.S. Cyber Command into U.S. Information Command to more fully leverage all available information capabilities in a synchronized manner in support of a whole-of-government approach to contesting adversaries in the information environment. See Nicholas J. Kane, "The Changing Character of War: Recommendations for DoD Reform to Compete with Russia in the Information Environment," Master's Thesis, Command and General Staff College, Fort Leavenworth, KS, 2018, 83.

51 Paul M. Nakasone, "An Interview with Paul M. Nakasone," *Joint Forces Quarterly*, no. 92 (1st Quarter 2019): 4-9, 6.

52 Ibid.